UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/403,689	10/22/1999	BERND KOWALSKI	2345/97	7576

26646 7590 10/13/2009

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
10/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/403,689	KOWALSKI ET AL.	
	Examiner	Art Unit	
	CHRISTOPHER J. BROWN	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The Request for Continued Examination has been entered and accepted.

Response to Arguments

The examiner has incorporated Dunn US 6,169,805 to teach a channel separate from a message transmission path.

Applicants arguments regarding a variable parameter having a length which is a function of the defined key length are unpersuasive because no support can be found in the instant specification to support the claim language. The rejection currently used length to define the variable, but uses the Vernam key length rather than a cipher key length. Examiner contacted the applicant about this issue but did not get a chance to discuss the issue. Nothing in the specification states that the variable parameter is a function of the defined key length.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which

it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 8, 15, 18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The claims state that the Vernam key is generated by a symmetrical cipher, where the variable parameter is a function of the secret key's defined key length.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson US 5,805,204 in view of Powar US 6,285,991 in view of Dunn US 6,169,805

As per claims 8 , 18, and 19, Thompson teaches generating a Vernam key (seed key) via a symmetrical cipher (DES), the generating being aided by using a secret key (imbedded key) and a variable parameter (random number) or seed) (

encrypting the generated random number using DES and the imbedded key to create a seed key) (Col 7 lines 18-28) It is well known that a Vemam key contains the properties of having a length that is equal to a length of a message to be protected, the secret key having a defined key length (64 bit DES), the variable parameter having a length which is a function of the defined key length (length of message). Thompson teaches encrypting, the message(teaches encrypting actual transmitted data using the seed key) (Col 7 lines 25-30). Thompson does not specify the Vernam cipher but only an "algorithm". The examiner asserts that the Vernam cipher is well known in the art (shown in the Handbook of Applied Cryptography page 21 by Menezes)

Thompson teaches communicating, from a sending point to a receiving point, a secret key ID (imbedded key ID) and the variable parameter (random number) (transmit the key ID and random number).

Thompson teaches regenerating the Vernam key (encrypting the random number using the imbedded key) (Col 7 lines 37-45).

Thompson teaches a storage space and one of a symmetrical cipher in a crypto-module, the crypto-module being separate from an encryptor (a smart card implements the DES algorithm to create the seed key) (Col 7 lines 40-45).

Thompson teaches performing encryption operations via the Vemam cipher in the encryptor (teaches performing decryption of the data using the seed key then passing the sseed key to the microprocessor which performs decryption) (Col 7 lines 40-51).

Thompson fails to teach sending the key and random number via at least one of (A) a secure channel separate from a message- transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher; regenerating the Vernam key; and decrypting the message.

Powar teaches sending data including a key via a message transmission path secured via an asymmetrical cipher (encrypting data and a session key with the public key of the customer, the customer using the private key to recover the session key, and the session key to decrypt data) (Col 4 line 62 to Col 5 line 13).

It would have been obvious to one of ordinary skill in the art to use the asymmetric encryption of Powar with the system because it provides privacy and security.

Dunn teaches that an encryption key and message are transmitted on different channels and paths, (Col 4 lines 40-45).

It would have been obvious to use Dunn with the invention to increase the security against key interceptionl.

As per claims 9-11 The examiner asserts the Vernam cipher is well known in the art as a very simple EXOR operation and is used for its simplicity and ease of use as shown in the Handbook of Applied Cryptography page 21 by Menezes. (Previously Presented).

As per claim 12 Thompson teaches storing the Vernam key (seed key) in the

storage space (not explicitly stated, the smart card stores "imbedded keys", so the smart card contains memory, and the card creates the vernam key, so it is stored upon creation). Thompson teaches the external crypto module being separate from the encryptor (Fig 7, smart card 11) Thompson teaches the encryptor includes at least one of a chip card, a multifunctional PC interface adapter and a PCMCIA module (smart card) (Col 7 lines 34-36).

Thompson teaches performing Vernam cipher operations exclusively in the encryptor, wherein the encrvptor includes including at least one of a chip card, a multifunctional PC interface adapter and a PCMCIA module (smart card is connected to encryptor where the vernam/seed key is passed and microprocessor decrypts data).

As per claim 13 Thompson teaches the crvpto-module is an external crypto-module (smart card) (Col 7 lines 35-40). Thompson teaches the external crypto module being separate from the encryptor (Fig 7, smart card 11) Thompson teaches controlling, via the Vernam cipher, encryption operations in the encryptor (smart card creates the seed key used for encryption operations in the encryptor)(Col 7 lines 37-45).

As per claim 14 Thompson teaches the Vernam key is stored in the encryptor (the seed key is passed to the encryptor)(Col 7 lines 42-47).

As per claim 15, Thompson teaches generating a Vernam key (seed key) via a symmetrical cipher (DES), the generating being aided by using a secret key

(imbedded key) and a variable parameter (random number) or seed) (encrypting the generated random number using DES and the imbedded key to create a seed key) (Col 7 lines 18-28) It is well known that a Vemam key contains the properties of having a length that is equal to a length of a message to be protected, the secret key having a defined key length (64 bit DES), the variable parameter having a length which is a function of the defined key length (length of message). Thompson teaches encrypting, the message(teaches encrypting actual transmitted data using the seed key) (Col 7 lines 25-30). Thompson does not specify the Vernam cipher but only an "algorithm". The examiner asserts that the Vernam cipher is well known in the art (shown in the Handbook of Applied Cryptography page 21 by Menezes)

Thompson teaches communicating, from a sending point to a receiving point, a secret key ID (imbedded key ID) and the variable parameter (random number) (transmit the key ID and random number).

Thompson teaches regenerating the Vernam key (encrypting the random number using the Imbedded key) (Col 7 lines 37-45).

Thompson teaches a storage space and one of a symmetrical cipher in a crypto-module, the crypto-module being separate from an encryptor (a smart card implements the DES algorithm to create the seed key) (Col 7 lines 40-45).

Thompson teaches performing encryption operations via the Vemam cipher in the encryptor (teaches performing decryption of the data using the seed key then passing the sseed key to the microprocessor which performs decryption) (Col 7 lines 40-51).

Thompson teaches the encryptor being capable of coupling to the crypto-hardware (decoder couples to smartcard, Fig 7) Thompson teaches the encryptor including at least one of a personal computer, software and a terminal which implements a Vemam cipher for broad-band applications in software (subscriber unit uses terminal to decrypt data, (Col 7 lines 32-52).

Thompson fails to teach sending the key and random number via at least one of (A) a secure channel separate from a message- transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher; regenerating the Vernam key; and decrypting the message.

Powar teaches sending data including a key via a message transmission path secured via an asymmetrical cipher (encrypting data and a session key with the public key of the customer, the customer using the private key to recover the session key, and the session key to decrypt data) (Col 4 line 62 to Col 5 line 13).

It would have been obvious to one of ordinary skill in the art to use the asymmetric encryption of Powar with the system because it provides privacy and security.

Dunn teaches that an encryption key and message are transmitted on different channels and paths, (Col 4 lines 40-45).

It would have been obvious to use Dunn with the invention to increase the security against key interceptionl.

As per claims 16, and 17, Thompson teaches crypto-hardware (smartcard) and

terminal having an intermediate storage storing the Vernam key (smart card creates the key, thus must store it, and passes a copy to terminal for utilization) (Col 7 lines 35-50).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 10/12/09
Primary Examiner, Art Unit 2439